Docket No. GFP108US **H1246**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re **PATENT** application of:

Applicant:	Marufa Kaniz
Application No.:	10/816,661
For:	METHODS AND APPARATUS FOR PASSING INITIALIZATION VECTOR INFORMATION FROM SOFTWARE TO HARDWARE TO PERFORM IPSEC ENCRYPTION OPERATION
Filing Date:	April 2, 2004
Examiner:	Yonas A Bayou
Art Unit:	2434

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants submit this brief in connection with the appeal of the above-identified case.

I. Real Party in Interest (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in the present appeal is GlobalFoundries.

II. Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))

Appellant, appellant's legal representatives, and/or the assignee of the present application are unaware of any appeals or interferences which will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-6, 8-12, and 14-23 are pending. Claims 7 and 13 are cancelled. Claims 1-6, 8-12, and 14 have been allowed. Claims 15-23 have been rejected. The rejection of claims 15-23 is appealed.

IV. Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv))

No claim amendments were made after the final rejection mailed November 16, 2009.

V. Summary of Claimed Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

According to the invention of independent claim 15 and referring generally to Fig. 1G, a method of encrypting outgoing data in a network interface system is claimed. (*See, e.g.,* p. 16, ln. 30 – p. 17, ln. 1). The method comprises providing initialization vector information 191 from a descriptor to a security system 124 in a network interface system 2 (element 43). (*See*, p. 17, lns. 10-14). Outgoing data is selectively encrypted or authenticated using the security system 124. (*See, e.g.,* p. 6, lns. 17-26). Outgoing data is selectively encrypted according to an initialization vector (IV) comprising an initial random data string from the outgoing data, before security information has been received by the security system 124. (*See,* p. 15, ln 18 – p. 16, ln. 15). The initialization vector from the outgoing data is employed to perform CBC encryption or authentication of the outgoing data according to the initialization vector information (element 46). (*See,* p. 17, lns. 23-25).

VI. Grounds of Rejection to be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))

Claims 15-23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,003,118 B1 (Yang et al.) in view of U.S. Patent No. 6,418,130 B1 (Cheng et al.).

Reversal of these rejections is respectfully requested.

VII. Argument (37 C.F.R. § 41.37(c)(1)(vii))

A. REJECTION OF CLAIMS 15-23 UNDER 35 U.S.C. § 103(a)

Claims 15-23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,003,118 B1 (Yang et al.) in view of U.S. Patent No. 6,418,130 B1(Cheng et al.). Withdrawal of the rejection is respectfully requested for at least the following reasons.

i. The rejection of claim 15 appears to be inconsistent with the allowance of claim 1.

The Final Office Action of 11/16/09 rejected claims 1 and 15 under 35 U.S.C. §103(a) as being unpatentable over the same prior art, Yang et al. in view of Cheng et al. (*See*, pp. 4-6). Upon receiving an Advisory Action affirming the rejection on 1/26/10, the applicant filed a pre-appeal request for review. The applicant's pre-appeal brief resulted in a decision by the pre-appeal brief conference panel to allow independent claim 1, and claims dependent therefrom, but to maintain the rejection of independent claim 15, and claims dependent therefrom. As will be more fully appreciated below, because the limitations of rejected claim 15 are analogous to the limitations of allowed claim 1, the ***rejection of claims 15-23 appears inconsistent with the allowance of claims 1-6, 8-12, and 14.***

In particular, independent claim 1 recites a network interface system comprising:

> (a) a security system coupled with a memory system, the security system being adapted to selectively encrypt outgoing data and to selectively decrypt incoming data; and
>
> (b) a descriptor management system being adapted to obtain initialization vector information from a host system and to provide the initialization vector information to the security system;
>
> ***(c) wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.***

Similarly, independent claim 15 recites a method of encrypting outgoing data in a network interface system, comprising:

> (a) selectively encrypting or authenticating outgoing data using the security system;
>
> (b) providing initialization vector information from a descriptor to a security system in a network interface system; and
>
> ***(c) selectively encrypting outgoing data according to an initialization vector (IV) comprising an initial random data string from the outgoing data, before security association information has been retrieved by the security system.***

In response to the Advisory Action of 1/26/10 the applicant made three arguments applicable to both claims 1 and 15. The applicant argued that the cited art ***fails*** to teach; (1) a security system adapted to employ an initial random data string, (2) that the initial random data string is from outgoing data, and (3) that the initial random data string begins encryption before security association information has been retrieved. These arguments are reiterated below in sections *ii – iv*.

Because the applicant's three arguments are equally applicable to both claims 1 and 15, the allowance of claim 1 should also be dispositive regarding the patentability of claim 15. Accordingly, applicant respectfully requests a reversal of the rejection of claim 15, and claims dependent therefrom.

In an interview with the Examiner conducted on May 28, 2010, the Applicant made an inquiry regarding the apparent inconsistency between the allowance of structure claim 1 and the rejection of analogous method claim 15. The Examiner however stated that the status of the applicant prevented him from commenting on the application and that instead the Board of Patent Appeals and Interference had to resolve any alleged inconsistency.

ii. The cited art does not teach a security system that is adapted to employ an initial random data string from outgoing data to begin encryption, as recited in claim 15.

Claim 15 recites a method of encrypting outgoing data in a network interface system comprising selectively employing an initialization vector, comprising an ***initial random data string*** from outgoing data. The Office Action concedes that Yang does not teach such a security system, but instead alleges that Cheng teaches a security system adapted to employ an initial random data string. (*See, O.A. of 11/16/09*, p. 6, lns. 4-10). However, as will be more fully appreciated below, Chang fails to teach a security system adapted to employ an ***initial random data string*** from outgoing data to begin encryption, as recited in claim 15.

More particularly, Cheng teaches a wireless communication system configured to reuse, rather than renegotiate, security associations (SAs). The Advisory Action of 1/26/10 notes, as illustrated in Fig. 4 where SA attributes are transferred from SU_k to SU_{k+1}, that the transferred SA attributes include transferring a last IKE phase 1 CBC output block prior to hand over, which is used as the initialization vector for encryption of the first IP packet subsequent to hand over. (*See, Cheng*, col. 6, lns. 61-63). In other words, an IKE phase 1 CBC block, calculated for SU_k is transferred to SU_{k+1} to be used as an initialization vector, so that an initialization vector does not have to be recalculated.

Accordingly, Cheng teaches a method of "***reusing previously established security associations*** [between MU and SU_k] to support newly formed connections between the MU (mobile unit) and SU_{k+1}" to avoid renegotiating SAs each time an MU changes its point of connection. (*See*, Col. 3, lns. 53-61). However, the term "***re-using***" means that the SAs were ***previously negotiated***. Since a previously negotiated SA is not ***an initial random data string***, Cheng does not teach an initial random data string, as recited in claim 15. Accordingly, for at least this reason, applicant respectfully requests withdrawal of the rejection of claim 15, and the claims which depend therefrom.

iii. The cited art does not teach a security system that is adapted to employ an initial random data string from outgoing data to begin encryption, as recited in claim 15.

Claim 15 recites a method of encrypting outgoing data in a network interface system comprising selectively employing an initialization vector (IV), comprising an initial random data string from outgoing data. The Office Action concedes that Yang does not teach such a security system, but instead alleges that Cheng teaches a security system adapted to employ an initial random data string from outgoing data. (*See, O.A. of 11/16/09*, p. 6, lns. 4-10). However, as will be more fully appreciated below, Cheng fails to teach a security system adapted to employ ***an initial random data string from outgoing data***, as recited in claim 15.

As stated above, Cheng teaches a wireless communication system configured to reuse security associations (SAs). In particular, Cheng notes that SU_k, upon receiving a request from SU_{k+1}, sends a reply message containing information necessary to define the ISAKMP SA attribute (comprising CBC output block). (*See*, col. 6, lns. 45-63). Therefore, the CBC output block (associated with claimed initialization vector) ***is part of the reply message sent from SU_{k+1} to SU_k***. However, the reply vector is only relayed between SU_k and SU_{k+1} and ***does not comprise outgoing data***. Because the reply vector does not comprise outgoing data, the CBC block (initialization vector), as taught by Cheng, is not a data string ***from outgoing data***, as recited in claims 1 and 15, but rather is only from a reply message sent between stationary units. Accordingly, for at least this additional reason, applicant respectfully requests withdrawal of the rejection of claim 15, and the claims which depend therefrom.

iv. The cited art fails to teach a security system adapted to employ an initial random data string from outgoing data to begin encryption before security association information has been retrieved by a security system, as recited in claim 15.

Claim 15 recites a method for encrypting outgoing data in a network interface system comprising encrypting outgoing data before security association information has been retrieved by the security system. The Office Action concedes that Yang does not

teach this limitation, but instead alleges that Cheng teaches "the security system is adapted to employ an initial random data string from the outgoing data ***to begin encryption before security association information has been retrieved*** by the security system." (*See, O.A. of 11/16/09*, p. 4, par. 5 – p. 5 par. 1). However, as will be more fully appreciated below, Cheng does not teach this limitation of claim 15.

Cheng describes in par. 1:48-60 that ISAKMP SAs are negotiated in Phase 1 before negotiating IPsec SAs and subsequent encryption in Phase 2. That is, the two phases are ***not independent***. Thus, Cheng teaches that a negotiated SA takes place in both phases 1 and 2 ***before encryption in phase 2***. (*See, e.g.,* col. 7, lns. 7-11; stating "the first time a MU connects to any SU in a given administrative domain, an IKE phase 1 negotiation and an IKE phase 2 negotiation must be accomplished, thereby establishing the ISAKMP SA and the IP_{SEC} SAs respectively."). Therefore, Cheng does not teach employing an initial random data string from the outgoing data to begin encryption ***before SA information has been retrieved*** by the security system.

Further, Cheng relies upon ***reusing previously established security associations*** to support these newly formed connections between MU and SU_{k+1}. However, in order to ***re-use*** **an SA**, Cheng ***must first have previously negotiated*** the SA, which can then be re-used in a subsequent hand-over.

By contrast, the claimed security system is adapted to begin encryption ***before*** security association information has been retrieved. Since, the claimed security system begins encryption before retrieving an SA, in contrast to the teaching of Cheng which first establishes an SA before it can be "re-used" to begin encryption in an IPsec phase II, Cheng fails to teach over the claimed invention. Accordingly, for at least this additional reason, applicant respectfully requests withdrawal of the rejection of claim 15, and the claims which depend therefrom.

B. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of the pending claims be reversed.

For any extra fees or any underpayment of fees for filing of this Brief, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, GFP108US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

/Thomas G. Eschweiler/
Thomas G. Eschweiler
Registration No. 36,981

National City Bank Building
629 Euclid Ave., Suite 1000
Cleveland, Ohio 44114
(216) 502-0600

VIII. Claims Appendix (37 C.F.R. § 41.37(c)(1)(viii))

1. (Previously presented): A network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising:

a bus interface system adapted to be coupled with a host bus in the host system and transfer data between the network interface system and the host system;

a media access control system adapted to be coupled with the network and to transfer data between the network interface system and the network;

a memory system coupled with the bus interface system and the media access control system, the memory system being adapted to store incoming and outgoing data being transferred between the network and the host system;

a security system coupled with the memory system, the security system being adapted to selectively encrypt outgoing data and to selectively decrypt incoming data; and

a descriptor management system coupled with the bus interface system and the security system, the descriptor management system being adapted to obtain initialization vector information from the host system and to provide the initialization vector information to the security system;

wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.

2. (Original): The system of claim 1, wherein the security system comprises at least one transmit security processor adapted to selectively encrypt or selectively authenticate the outgoing data.

3. (Original): The system of claim 2, wherein the initialization vector information indicates whether the outgoing data is to undergo cipher block chaining (CBC) encryption in the security system.

4. (Previously presented): The system of claim 3, wherein the at least one transmit security processor selectively employs an initialization vector (IV) comprising the initial random data string from the outgoing data to perform CBC encryption according to the initialization vector information from the descriptor management system.

5. (Original): The system of claim 4, wherein the at least one transmit security processor employs the initialization vector (IV) from the outgoing data if the initialization vector information indicates that the outgoing data is to undergo cipher block chaining (CBC) encryption.

6. (Original): The system of claim 4, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

7. (Canceled):

8. (Original): The system of claim 3, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

9. (Original): The system of claim 1, wherein the initialization vector information indicates whether the outgoing data is to undergo cipher block chaining (CBC) encryption in the security system.

10. (Previously presented): The system of claim 9, wherein the security system selectively employs an initialization vector (IV) comprising the initial random data string from the outgoing data to perform CBC encryption according to the initialization vector information, and wherein the security system is adapted to use the initial random data string as a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.

11. (Previously presented): The system of claim 8, wherein the security system selectively employs the initialization vector (IV) comprising the initial random data string used as a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.

12. (Original): The system of claim 10, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

13. (Canceled):

14. (Original): The system of claim 1, wherein the initialization vector information indicates a length of an initialization vector in the outgoing data.

15. (Previously presented): A method of encrypting outgoing data in a network interface system, the method comprising:

providing initialization vector information from a descriptor to a security system in a network interface system;

selectively encrypting outgoing data according to an initialization vector (IV) comprising an initial random data string from the outgoing data, before security association information has been retrieved by the security system;

selectively encrypting or authenticating outgoing data using the security system; and

selectively employing the initialization vector (IV) from the outgoing data to perform CBC encryption or authentication of the outgoing data according to the initialization vector information.

16. (Original): The method of claim 15, wherein providing the initialization vector information comprises:

reading a transmit descriptor from a host system; and

providing initialization vector information from the transmit descriptor to the security system.

17. (Original): The method of claim 16, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information whether an initialization vector is present in the outgoing data.

18. (Original): The method of claim 17, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption further comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

19. (Original): The method of claim 16, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

20. (Original): The method of claim 15, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information whether an initialization vector is present in the outgoing data.

21. (Original): The method of claim 20, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption further comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

22. (Original): The method of claim 15, wherein selectively employing an initialization vector from the outgoing data to perform CBC encryption comprises determining from the initialization vector information a length of an initialization vector in the outgoing data.

23. (Previously presented): The method of claim 15, further comprising employing the initial random data string as a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.

IX. Evidence Appendix (37 C.F.R. § 41.37(c)(1)(ix))

No additional evidence not already part of the official record is relied upon in the arguments provided herein.

X. Related Proceedings Appendix (37 C.F.R. § 41.37(c)(1)(x))

Not applicable.